Implementation Instructions for DAA Participants to WebChoices

Confidential

Implementation instructions for DAA Participants from the "the choice page" to WebChoices.

WebChoices allows for the transparent and reliable setting of opt-out choice from data collection and use for IBA across the major browsers.

The new feature set in WebChoices is particularly relevant when companies use non-third party cookies (First-Party Cookies) or cookie-less[1]/non-cookie technologies for interest-based advertising ("IBA") (collectively "non-cookie technologies"). Companies using non-cookie tech should integrate with the WebChoices as it makes setting opt outs more transparent and allows opt outs to be set in more cases than in the current version.

If your company does NOT engage in third-party IBA using non-cookie technologies, then you do not need to manually integrate with this tool, as migration from the current choice page to WebChoices will occur automatically. However, you may need to whitelist the new subdomain - optout.aboutads.info.

Links to access the WebChoices Tool should point to optout.aboutads.info.

CONFIDENTIAL - DO NOT FORWARD OR SHARE

[1] Cookie-less technologies in this WebChoices document do NOT include IDFA, AAID. DAA offers a different tool, AppChoices, for consumers to set preferences in the in-app environment. AppChoices is available to consumers in iOS, Android and Amazon app stores for free.

WebChoices

Centralized Consumer Opt-Out Platform

PUBLISHED/UPDATED March 6, 2017

This document describes how the opt-out platform works and how to integrate your company's opt-out infrastructure with the WebChoices tool.

This opt-out platform is backwards compatible with the DAA's old choice page.

Onboarding and Management
Companies currently listed on the existing choice page and companies who may choose to participate in the future, now will have available a new administration portal to upload and modify information about their company and their opt-out endpoints. Companies will no longer need to upload XML documents to provide information about their company and the location of the endpoints. Access and credentials for this portal will be sent shortly.

> The WebChoices tool resides at: optout.aboutads.info. <

Some links to access the WebChoices Tool point to www.aboutads.info/choices, the old URL for the DAA Choice Page. DAA will redirect to this sub domain.

This integration guide contains five sections:

I. CONSUMER OPT-OUT EXPERIENCE

The purpose of the WebChoices opt-out tool is to provide consumers with a destination to:

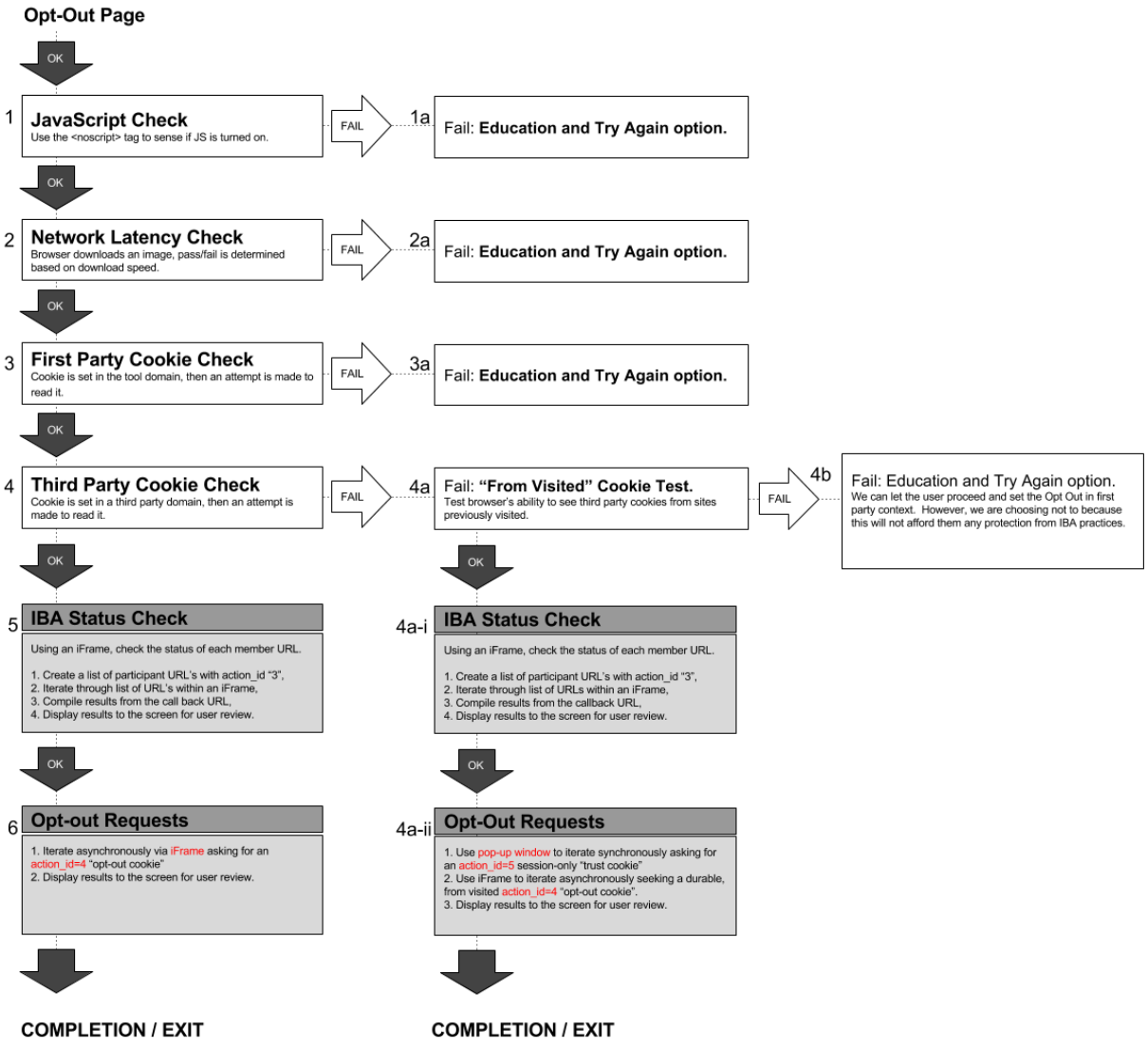
A. Identify a list of companies who have committed to conducting responsible advertising practices in alignment with the DAA's Principles;

B. Receive a detailed report of which companies engage in Interest-Based Advertising on a consumer's browser; and,

C. Provide consumers the ability to opt out of collection and use of data for Interest-Based Advertising from one, several, or all of the companies listed on the WebChoices tool.

D. The Opt-Out functionality flowchart demonstrates the high-level decision logic implemented by the new WebChoices opt-out platform. This is provided to help companies understand the structure of the new opt-out platform and to help them implement the WebChoices opt-out platform specifications.

Diagram: Opt-Out functionality Flowchart



II. ACCESS TO THE COMPANY INFORMATION ADMINISTRATION AREA

This section provides instructions on a company can access self-management administration area.

A. **Access**. WebChoices is accessible at the following URLs:

1. **For DAA Participants**
   a. Staging & Onboarding: http://staging.aboutads.info
   b. Production: http://optout.aboutads.info

B. **Credentials**. The staging environment is essentially a sandbox where companies' opt-out functionality can be tested without being released to the public. Access to the staging environment requires a password. All companies using the system will be required to provide this password twice - once for access to the HTTP portion of the system and once again for HTTPS portions of the system. The credentials are as follows:

1. **Username**: participant
2. **Password**: bc_2341cb

III. ONBOARDING PROCESS

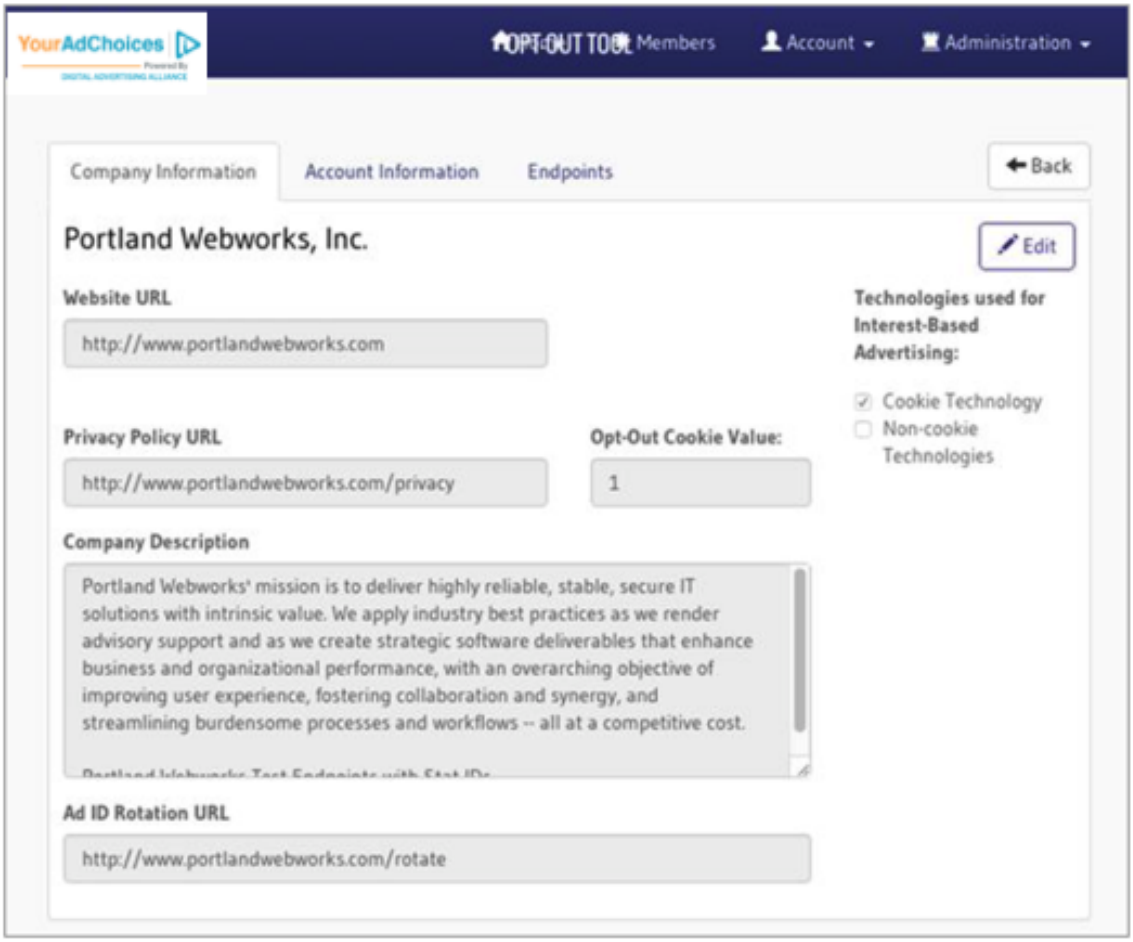
This section provides information on how companies can onboard their organization's information and endpoints to the WebChoices opt-out platform.

A. **Step 1 - Email Contact**: Each company currently listed on the current choice page will receive an email invitation to start the onboarding process. Please ensure that your designated point of contact ("POC") is aware of this email and has the necessary rights to start the onboarding process. While many companies use technical staff for this process, it is not required.

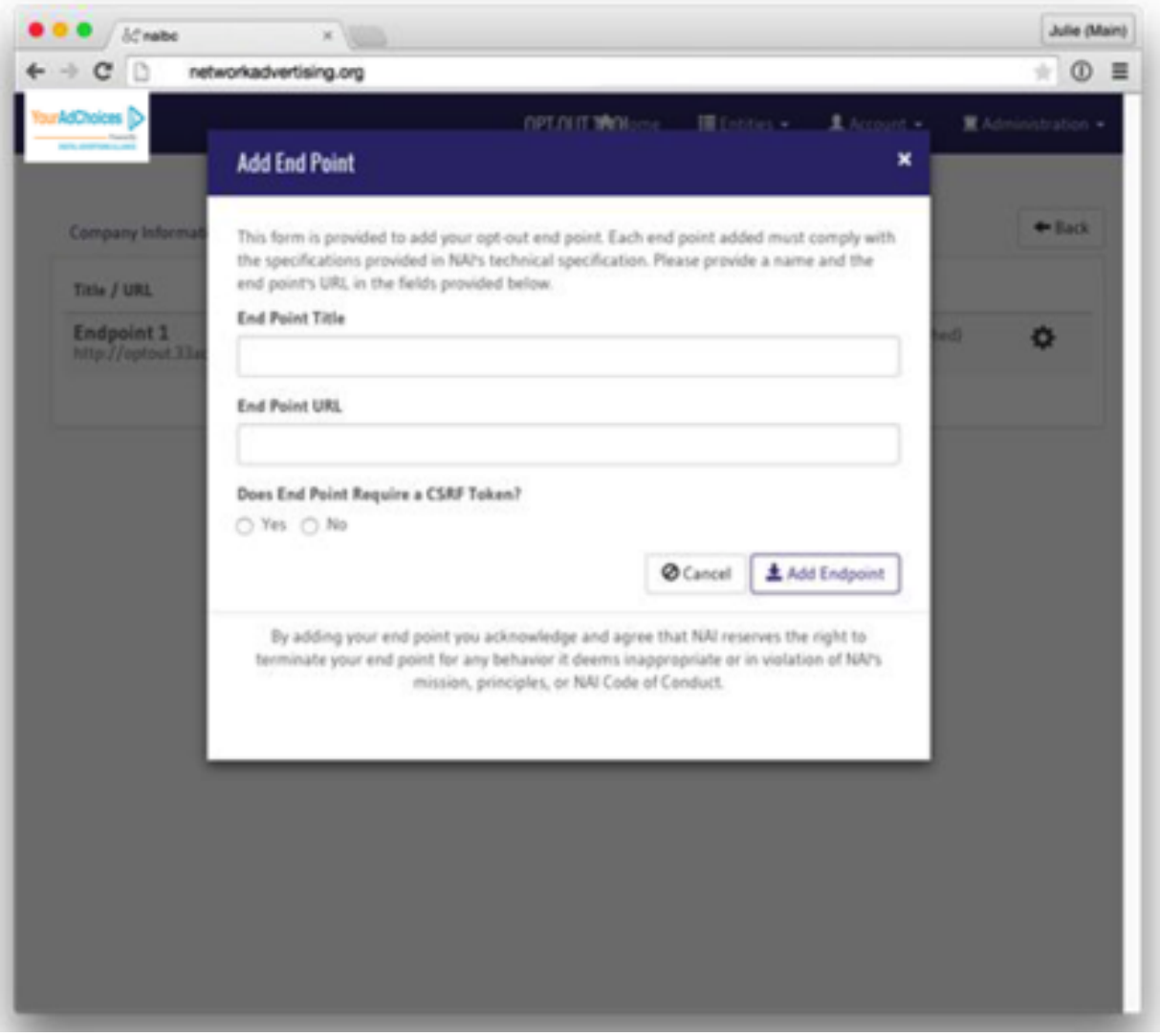
B. **Step 2 - Respond to Email**: Your organization's POC will receive an email from DAA to the email address you have provided. To update your contact email, please inform DAA staff directly.

C. **Step 3**: To fully activate your account, please set your account's password.

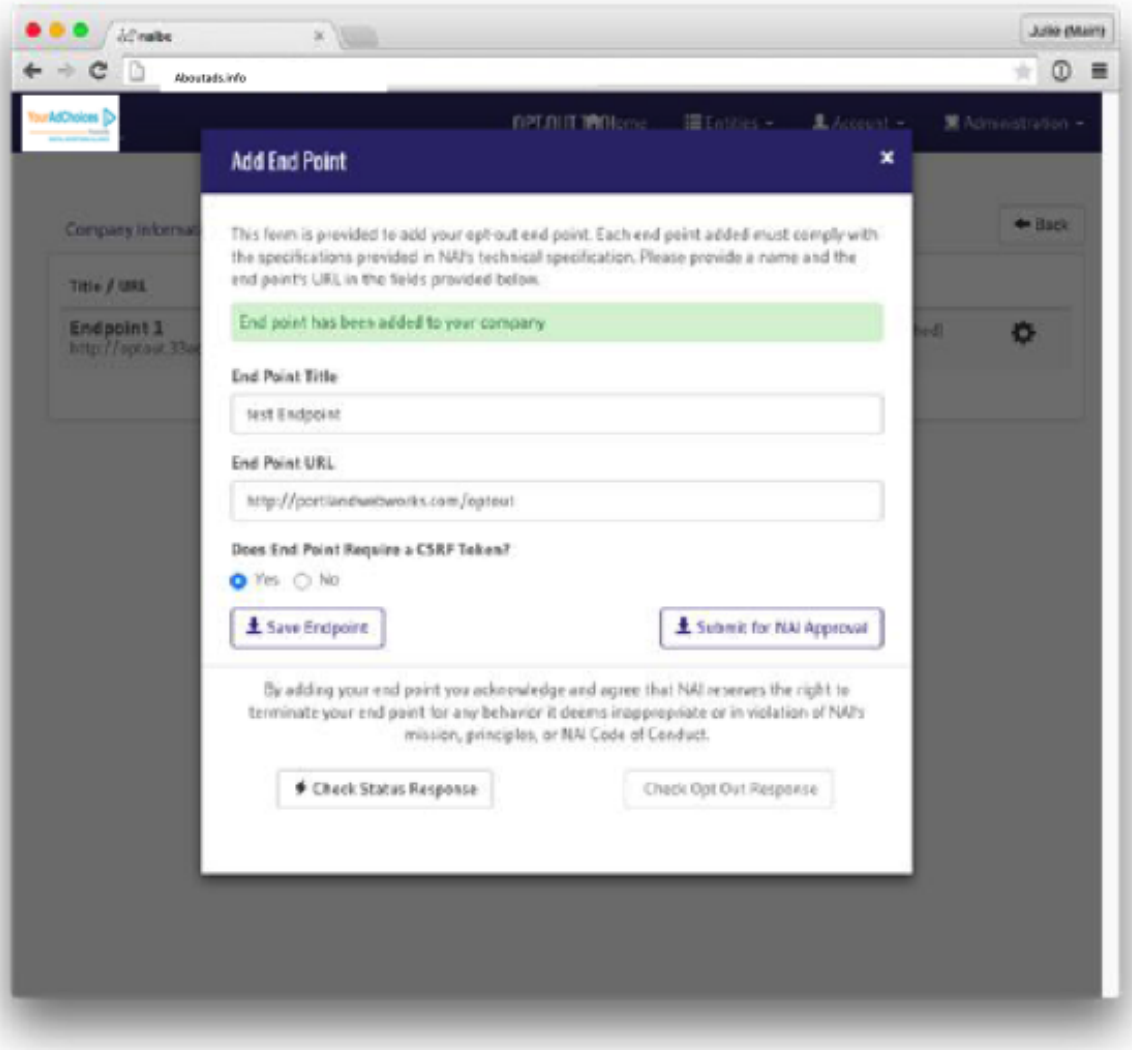
D. **Step 4**: After setting your password successfully, you will be presented with a screen to provide further information. On the following web-based form, provide the following.
    1. A URL to your organization's website;
    2. A URL to your organization's privacy policy or privacy notice;
    3. A brief description of your company (this will appear on the opt-out page);
    4. A designation of whether you use cookie technologies for IBA;
    5. A designation of whether you use non-cookie technologies for IBA;
    6. The (non-unique) value of your opt-out cookie; and,
    7. The URL where your Advertising ID rotation functionality exists. Companies who elect to extend consumer opt outs to both IBA **and** non-cookie technology Reporting activities are not required to provide a rotation mechanism.



E. **Step 5**: After clicking the “Endpoints” tab navigation option, provide the URL details associated with your opt-out infrastructure and click “Add Endpoint.” No changes will be published live on the production version of the page without DAA staff review and approval. Please end by clicking “Add Endpoint.”



F. **Step 6**: After selecting “Add Endpoint,” you will be given the option to perform a simple baseline test of the endpoint’s compatibility with the required specification. If the script passes this baseline test, submit it for review and approval by selecting “Submit for DAA Approval.” DAA staff will then review your endpoint and notify you of approval or with requests to repair any errors, if discovered.



G. **Step 7**: After DAA review of your submission, you will receive a confirmation email indicating that your endpoint has been approved and activated. DAA staff will then migrate the change to the production environment and your endpoint will be available to consumers. The WebChoices company portal provides up-time stats on all endpoints for the previous 7 days. As a best practice, please visit the “Endpoints” tab on a regular basis to view the uptime stats of your endpoints for the past 7 days.

IV. CONSUMER OPT-OUT INTEGRATION SPECIFICATION

This section describes what is required to implement a WebChoices Opt-Out Service Endpoint capable of integrating with the WebChoices consumer opt-out tool.

A. General Requirements

1. Browser Compatibility

a) No technologies shall be utilized in your implementation of an endpoint that will render it unable to function reliably and quickly on all major browser and operating system combinations on desktop and mobile devices.

2. P3P Headers

a) All endpoint responses must contain a valid P3P header string in the response. This header is required for Internet Explorer compatibility. Please review the Platform for Privacy Preferences (P3P) Project (http://www.w3.org/P3P/) for details regarding generation of and compliance with the P3P header specification. For example, a P3P Header looks like: “P3P: CP="BUS CUR CONo FIN IVDo ONL OUR PHY SAMo TELo"”

3. Opt-Out Cookies

a) Companies shall use generic values for their company's opt-out cookie value.

b) Opt-out cookies that are generated by a company endpoint shall have a minimum lifespan of 5 years and shall be renewed for at least another 5 years upon each subsequent opt-out request received. When calculating the 5-year lifespan, account for a possible two extra days to account for leap years.

c) Cookies not required to opt out a user shall never be set by a company’s WebChoices endpoint. Any cookies that are necessary for a company’s endpoints to function (e.g., tokens) shall not persist past the current browser session.

d) The WebChoices tool may give companies an enhanced trust relationship when “Action ID=5” is used to set a session cookie prior to setting an IBA opt-out cookie. After setting this opt-out cookie, the WebChoices tool is made available for companies to reliably set opt-out choices in third-party cookie blocking environments in the “From Visited” scenario. Consistent with DAA Principles, any use of technology (including cookies) may still be permissible so long as the data cannot be collected or used for IBA after an opt-out choice. Violating this requirement may result in a breach of the terms under which this tool is offered to companies.

e) Companies may not exploit the trusted relationship established via WebChoices tool. But companies may leverage their existing 1st party relationships or non-cookie technology for non-IBA purposes after opt out.

f) Some companies may have multiple endpoints, each with a different opt-out cookie value. Please contact DAA staff if you have multiple opt-out cookies with differing values.

g) Upon a successful opt out, all cookies related to IBA activities shall be expired, except those necessary to maintain the opt-out status of the consumer.

h) Non-cookie based IBA technologies, such as IBA made possible by a statistical identifier (Stat ID) or HTML5 local storage, must honor the presence of an opt-out cookie being set, regardless of non-cookie technology used.

4. Use of Optional Anti-CSRF Tokens

a) Companies are allowed (but not required) to exchange anti-CSRF tokens in advance of setting an opt-out cookie as part of this specification for a consumer opt-out process.

b) Companies seeking the additional transactions that allow the anti-CSRF token exchange may be asked to meet elevated performance SLA's (such as endpoint response times) for their endpoints to ensure that the company's additional transactions do not negatively impact usability for consumers.

c) If a request to an endpoint fails due to Anti-CSRF Token validation, the endpoint is required to return the appropriate error code back to the requestor and at no point shall it return rendered content or xml that is visible within a consumer's browser window.

d) The Anti-CSRF Token may impact the usability of action_ID=5 scenarios and is being considered for deprecation.

5. Opt Out Failures

a) As is the case with the current choice page, all failures/errors must return a result back for processing, regardless of reason. Any failure to do so may result in your endpoint being deactivated automatically to preserve a fast, accurate and predictable consumer experience. Companies will use reasonable efforts to cure issues raised by DAA. Failure to address issue within a reasonable may result in, at the discretion of DAA, delisting a company.

6. Recommendations

a) Use some variation of 'opt-out' as the name of your company's opt-out cookie. This helps consumers identify which cookies are opt-out cookies.

b) Use Request Referrers to limit access to a company's endpoint, but each one must permit requests from allowable subdomains including dev, integrate, qa, staging, www and optout. Overly restrictive referrer validation logic within a company's endpoint can interfere with critical quality assurance processes when onboarding new companies or when releasing new features to the opt-out tool.

7. Performance

a) Maintaining fast endpoints is becoming increasingly important with the implementation of additional technologies. There will be increased focus to ensure company endpoints are responding quickly to ensure a fast opt-out experience for users.

b) The recommended approach for those companies that are not using non-cookie technologies is to use a HTTP 302 redirects whenever possible. Endpoints that make use of JavaScript for browser redirection must particularly focus on browser compatibility and rapid response times. Each company endpoint has a limited amount of time to deliver a response and JavaScript (or chained redirects) can add undesirable processing time and possibly even result in a failure being reported to the consumer due to a company's endpoint not meeting a reasonable allowable transaction response time.

B. Status and Token

This response shall return the consumer's status with regards to the existence of an IBA identifier or opt-out. Status must be based on the presence of a cookie or non-cookie identifier that is used for IBA at the time such status is presented to the consumer.

1. Request

Attribute	Description / value
Referer	http://<dev | staging | qa | integrate | www | optout>.aboutads.info/*
Accept	text/html,application/xhtml+xml

Sample Requests URLs:
http://your.domain/with/path/to/endpoint
?action_id=3
&participant_id=10
&rd=http%3A%2F%2Fwww.aboutads.info
&nocache=223442

Field	Data Type	Description
action_id	integer	Value "3" indicates a status request and token if applicable
participant_id	string	Participant Identifier for the Opt-out tool to correlate your endpoint with operations. Value is subject to change without notice.
rd	string	hostname and protocol http://www.aboutads.info
nocache	string	Ignore: cache buster

2. Response (Legacy Specification)

This is the existing specification and can be used by companies that are utilizing ONLY cookie identifiers for IBA (i.e. companies NOT employing non-cookie tech).

Field	Data Type	Description
rd	string	**rd** value from request
participant_id	integer	**participant_id** value from request
status	integer	1 = No IBA cookie(s) from Participant on the browser. 2 = IBA cookie(s) from Participant present on the browser. 3 = Opt-out cookie is present on the browser.
token	string	optional Anti-CSRF string, Must be valid ASCII characters allowed in a URL.

Response URL:
<**rd**>/token/<**participant_id**>/<**status**>/<**token**>
Example:
http://www.aboutads.info/token/**123/1/magic_string**

3. Response (New Specification)

This response is required for participants. Companies utilizing non-cookie technologies are required to provide accurate status as specified below.

Field	Data Type	Description
rd	string	**rd** value from request
participant_id	integer	**participant_id** value from request
cookie-status	integer	0 = Not Applicable - Cookie Technologies are not in use 1 = No IBA cookie(s) from Participant on the browser 2 = IBA cookie(s) from Participant present on the browser. 3 = Opt-out cookie is present on the browser.
other-status	integer	0 = Not Applicable - Non-Cookie Technologies are not in use 1 = No Non-Cookie IBA Identifier from Participant present for the browser 2 = Non-Cookie IBA Identifier from Participant present for the browser. 3 = Non-Cookie Opt-out from Participant present for the browser.
token	string	optional Anti-CSRF string, Must be valid ASCII characters allowed in a URL.

Response URL:
<rd>/token/<participant_id>/**<cookie-status>-<other-status>**/<token>

Example for company using non-cookie technology:
http://www.aboutads.info/token/123/1-1/csrftoken

Example for company using only cookie technology:
http://www.aboutads.info/token/123/1**-0**/csrftoken

C. Opt Out

Opt out a consumer from the collection and use of data for IBA by setting an "opt-out" cookie on the consumer's browser. **This action reports success or failure and must be based on the actual presence of the opt-out cookie in the consumer's browser**. Verification of the presence of the "opt-out" cookie is usually accomplished by redirecting to a verification page or script before redirecting the result signal back to the WebChoices tool. If utilizing server-side non-cookie technologies (e.g., statistical identifiers), the opt out must also be persisted on the company's server.

1. Request

Attribute	Description / value
Referer	http://<dev | staging | qa | integrate | www | optout>.aboutads.info/*
Accept	text/html,application/xhtml+xml

Sample Requests URLs:
http://your.domain/endpoint
?action_id=4&participant_id=10
&rd=http://www.aboutads.info
&token=magic_value&nocache=223442

Field	Data Type	Description
action_id	integer	Value "4" indicates an opt out request
participant_id	string	Participant Identifier for the Opt-out tool to correlate your endpoint with operations. Value is subject to change without notice.
rd	string	hostname and protocol http://www.aboutads.info
token	string	optional Anti-CSRF string if returned during the status check
nocache	string	Ignore: cache buster

2. Response (Legacy Specification)

This is the existing specification and can continue to be used by companies that are utilizing only cookie-based identifiers for IBA purposes.

Field	Data Type	Description
rd	string	**rd** value from request
action_id	integer	**action_id** value from request
participant_id	string	**participant_id** value from request
result_id	integer	1 = **Success:** after an opt out attempt, the opt out cookie is present on the user's browser 2 = **Failure:** after an opt out attempt, the cookie is not present on the user's browser 3 = **Failure:** anti-CSRF token mismatch [4..] = Reserved for future use
message	string	optional simple ascii text string fully URL compliant.

Response URL:
<**rd**>/finish/<**participant_id**>/<**action_id**>/<**result_id**>/<**message**>

Example:
http://www.aboutads.info/finish/123/4/1/simple_string

3. Response (New Specification)

This response is required is for participants. Companies utilizing non-cookie technologies are required to provide accurate opt-out result as specified below.

Field	Data Type	Description
rd	string	**rd** value from request
action_id	integer	**action_id** value from request
participant_id	string	**participant_id** value from request
cookie-result	integer	0 = **Not Applicable** - Cookie technologies are not in use 1 = **Success:** after an opt out attempt, the opt out cookie is present on the user's browser 2 = **Failure:** after an opt out attempt, the cookie is not present on the user's browser 3 = **Failure:** anti-CSRF token mismatch [4..] = Reserved for future use
other-result	integer	0 = **Not Applicable** - Non-Cookie technologies are not in use 1 = **Opt Out Success**: Non Cookie Identifier for the browser has been received by the Participants server 2 = **Opt Out Failure**: Non Cookie Identifier for the browser was not received by the Participants server 3 = **Failure:** anti-CSRF token mismatch [4..] = Reserved for future use
message	string	optional simple ascii text string fully URL compliant.

Response URL:
<rd>/finish/<participant_id>/<action_id>/<cookie-result>-<other-result>/<message>

Example:
http://www.aboutads.info/token/**123/1-1/magic_string**

V. ESTABLISHING A FIRST PARTY TRUST RELATIONSHIP

This is a new feature available for all companies, regardless if they utilize cookies exclusively or also use non-cookie technologies for IBA. It is especially designed as a way to reliably set choice for non-cookie tech in third-party cookie-blocking environments, but all companies may use it to future-proof their choice systems or for other reasons, consistent with DAA Principles.

In order to support browsers that restrict setting cookies in third-party contexts, it has become necessary to add a new action_id to the existing action_ids currently required from participant endpoints.

This new request, known as action_id=5, is only used when a browser is configured to reject third-party cookies, but allows setting third-party cookies from sites “previously visited”. There is no callback request or verification and it is the company’s responsibility to maintain a responsive endpoint.

The purpose of this request is to set a session cookie so that a temporary trust relationship is created with the browser. Any cookies set during this process will be established in a first party context with your domain. This will allow the subsequent opt-out request (action_id=4) to set an opt-out cookie in a third-party context.

If the browser does not already have a first-party cookie set from the company’s domain, this will create a trust relationship with the browser that may not have been otherwise possible. If an enhanced trust relationship is created as a part of this process, you may need to indicate this in the cookie value. This will allow you to prevent your systems from setting any additional cookies (such as frequency capping, ad delivery & reporting) once an opt-out is set on browsers where an enhanced trust relationship exists.

A. Request

Headers

Attribute	Description / value
Referer	http://<dev | staging | qa | integrate | www | optout>.aboutads.info/*
Accept	text/html,application/xhtml+xml

Sample Requests URLs:
http://your.domain/endpoint?action_id=5&nocache=223442

URL Parameters

Field	Data Type	Description
action_id	string	value “5” indicates establish temporary trust by setting a session cookie.
nocache	string	Ignore: cache buster

B. Response

1. All cookies shall be set using HTTP headers. There is no redirect required as part of this request. **The use of JavaScript in this step is prohibited.**

C. Guidelines For using a Trust Cookie (session cookie)

1. The cookie for this step shall be a **session cookie with no expiration set.**

2. This cookie shall be separate from the opt-out cookie, IBA cookies, and Reporting cookies.

3. The cookie name and value shall be generic (non-unique). The best practice for this step shall be to use cookie name=“FPtrust” and cookie value=“1”

D. Guidelines for response

1. A company’s response shall be a single HTTP 200 response.

2. Company shall set cookies using HTTP headers. **The use of JavaScript is prohibited.**

3. No output shall be displayed to the screen unless for debugging purposes. This shall occur on: staging.aboutads.info AND NOT optout.aboutads.info

4. Company’s response time shall be below 250ms. Timeouts for this step are very low. To facilitate a positive user experience, it is important that an adequate response time be maintained on all company endpoints to ensure timely opt-out delivery to consumers’ browsers.

This document is the Confidential Information of the DAA and may only be used for the purposes of integrating with the WebChoices opt-out tool. It is subject to all confidentiality agreements between and among the DAA, you and your company. The information contained in this document may not be used to reverse-engineer, deconstruct, disassemble, or decompile any DAA software or the software of any other DAA Participant.